REMARKS

This is in response to the Office Action mailed on August 5, 2004 in which claims 1-136 were pending. Claims 1-15, 20-24, 28, 29, 32-42, 46-49, 53-70, 75-78, 82, 83, 86-103, 108-112, 116, 117, 120-128, and 130-136 were rejected under 35 U.S.C. 102(e) as being anticipated by Diamant et al., U.S. Pat. No. 6,268,789 ("the Diamant patent"). Claims 16-19, 25-28, 30, 31, 43-45, 50-52, 71-74, 79-81, 84, 85, 104-107, 113-115, 118, 119, and 129 were rejected under 35 U.S.C. §103(a) as being unpatentable over the Diamant patent in view of Aucsmith et al., U.S. Pat. No. 5,940,513 ("the Aucsmith patent"). In light of the arguments presented below, it will be apparent that all pending claims are allowable over the cited references. Reconsideration and notice to that effect is respectfully requested.

Applicant noted a clerical error in the preliminary amendment, which resulted in two claims 128 being submitted. The second claim 128 is amended herein to change the claim number to claim 137. Applicant notes that, due to the error, the claim fee of $18 for the additional claim was not paid with the preliminary amendment filed on July 18, 2003. The Director is hereby authorized to charge the additional claim fee associated with this paper to Deposit Account No. 23-1123.

Additionally, applicant noted a typographical error in claim 131 wherein the phrase "of the" was repeated. With this Amendment, the phrase "of the" is deleted from claim 131. No substantive change is made to the text of the claim.

In the Office Action, all of claims 1-136 were rejected over the Diamant patent either alone or in combination with the Aucsmith patent. However, the Diamant patent does not teach, suggest or disclose all the elements of the present invention, and is more appropriately understood as an example of the prior art discussed at page 2 of the present application.

The Diamant patent discloses a device for protecting secured areas in a computer system, which includes a storage unit divided into two storage areas. The Diamant patent discloses a managing controller 98 that controls access to both the public storage area 16 and secured storage area 18 of the storage unit 14 via input/output interface 96, and that the managing controller 98, which is part of server 4 (in FIG. 2), "stores" the information in one or both areas (see Col. 7, line 60 through Col. 8, line 25).

In general, the Diamant patent refers to a conventional computer security system such as that described at page 2 of the application. Such a system is flawed because the security device operates in an environment that is common to the operating system.

> "Perhaps the greatest fundamental problem with conventional computer security systems is that their operation is common to the environment of the operating system environment. Furthermore, the operating system environment for many computer systems is also common to the Internet environment, for example, or another network communications medium. Because of this common environment, many means of attack on a computer system are available merely by moving computer code from the Internet to the computer operating system."

(See page 2, lines 1-7 (emphasis added)). The managing controller 98 of the Diamant patent is external to the storage unit 14 and is coupled to a secured network 8 and to a public network 6, which "is also connected to an external network which in the present example is the Internet 80" (See the Diamant patent, Col. 5, lines 36-37). The managing controller 98 exists in an environment common to the operating system environment, which is common to the Internet environment. Consequently, the managing controller 98 is susceptible to attack by moving computer code from the Internet to the operating system of the server 4.

Rejections under 35 U.S.C. §102(e)

In the Office Action, claims 1-15, 20-24, 28, 29, 32-42, 46-49, 53-70, 75-78, 82, 83, 86-103, 108-112, 116, 117, 120-128, and 130-136 were rejected under 35 U.S.C. 102(e) as being anticipated by the Diamant patent. The cited claims include each of independent claims 1, 35, 56, 89, 123, and 132, and dependent claims that depend from the independent claims.

Referring now to the method claims of the present invention, independent claim 132 reads as follows:

> A method for promoting security in a computer system having an operating system in operative connection with a storage device, wherein said storage device includes a processor and firmware for processing data stored on the storage device, the method comprising:
>> partitioning a storage medium of the storage device into a data partition and a secure data partition, the data partition being accessible to a user and the secure data partition being invisible to the user, <u>the secure data partition for storing</u> secure data <u>and one or more authority records</u>; and
>> <u>restricting access to the secure data partition such that only the firmware may access the secure data and the one or more authority records</u>.

(emphasis added). The Diamant patent does not teach, suggest or disclose "a secure data partition for storing … one or more authority records" as recited in the claim. The Diamant patent makes no mention of authority records as taught by the claimed invention. Moreover, the Diamant patent does not teach, suggest or disclose the claimed recitation of "restricting access to the secure data partition such that only the firmware may access the secure data and the one or more authority records" as recited in the claim.   In fact, the Diamant patent teaches controlling access to the secure storage area using an external controller via an interface between the external controller and the storage device (See, for example, lines in Fig. 1 connecting controller 12 to storage device 14; see I/O 1120 in FIG. 14 connecting

controlling device 1100 to storage device 1124). The controlling device is shown either operating from within the operating system environment of the server 4 (for example, in FIG. 1), or operating as a stand alone device external to the storage device. In either case, the controlling device does not restrict access such that "only the firmware may access the secure data and the one or more authority records" as the claim recites. Therefore, the Diamant patent does not teach, suggest or disclose all the elements of independent claim 123.

Independent method claim 1 includes "a security partition having at least one authority record and at least one data set associated with said authority record" and "limiting access to the security partition of said storage device by said operating system of said computer system". The Diamant patent does not teach, suggest or disclose authority records or the "at least one data set associated with said authority record" as recited in claim 1. Additionally, the Diamant patent does not teach, suggest or disclose "limiting access to the security partition of said storage device by said operating system" as recited in claim 1. Instead, the Diamant patent introduces an external controller element, which operates within the same environment as the operating system for controlling access to the security partition. The Diamant patent makes no mention of "limiting access" "by the operating system" as recited in the claim, and, in fact, the controller element of the Diamant patent controls access to the storage device partitions from within the operating system of the server, therby allowing access by the server's operating system to the partition. The Diamant patent is concerned with limiting access by remote nodes (Ref. Numerals 20, 30 and 40 in FIG. 1, for example) based on their network connections (e.g. public network 6 or secured network 8) *(See* Col. 5, line 25 through Col. 6, line 54), rather than access by the operating system. The Diamant patent does not teach, suggest

or disclose "at least one authority record and at least one data set associated with said authority record" or "limiting access to the security partition of said storage device by said operating system of said computer system" as recited in independent claim 1.   Therefore, independent claim 1 is allowable over the cited reference.

Referring now to the apparatus claims of the present invention, independent claim 123 reads as follows:

> 123. (Previously Added) A storage device for promoting security in a computer system, the storage device comprising:
> a storage medium for storing data;
> firmware for reading data from and writing data to the storage medium; and
> a partition defined on the storage medium for dividing the storage medium into a data partition and a secure data partition, the secure data partition for storing secure data and one or more authority records;
> wherein only the firmware is permitted to access the secure data and the one or more authority records.

(emphasis added).   The Diamant patent does not teach, suggest or disclose "a secure data partition for storing … one or more authority records" as recited in claim 123.   The Diamant patent makes no mention of authority records as taught by the claimed invention.   Moreover, the Diamant patent does not teach, suggest or disclose limiting access to the secure data and the one or more authority records such that "only the firmware", which is part of the storage device, "is permitted access" as recited in the claim.   As previously discussed, the Diamant patent teaches controlling access to the secure storage area using an external controller within the operating system environment of the server 4 (for example, in FIG. 1). Since the external controller operates within the operating system environment of the server 4, the Diamant patent teaches away from the claimed invention, where "only the firmware of the storage device is permitted to access

the secure data and the one or more authority records" as recited in the claim. Therefore, the Diamant patent does not teach, suggest or disclose "firmware for reading data from and writing data to the storage medium" or authority records" as recited by the claims. Moreover, the Diamant patent does not teach, or disclose a storage device "wherein only the firmware is permitted to access the secure data and the one or more authority records" as recited by independent claim 123.

Independent claims 35, 56, and 89 include "a security partition having at least one authority record and at least one data set associated with said authority record" and "limiting access to the security partition [or a portion of the storage device] of said storage device by said operating system of said computer system." As previously discussed, the Diamant patent does not teach, suggest or disclose authority records or the "at least one data set associated with said authority record" as recited by the claims. Additionally, the Diamant patent does not teach, suggest or disclose "limiting access to the security partition of said storage device by said operating system" according to the claimed invention. Instead, the external controller of the Diamant patent operates within the same operating system environment as the server. Thus, the Diamant patent teaches away from the claimed invention where access to the security partition by the operating system is limited. The Diamant patent does not teach, suggest or disclose an "authority record", "at least one data set associated with said authority record", "limiting access to the security partition [or a portion]" of the storage device "by the operating system" as recited by independent claims 35, 56, and 89. Therefore, independent claims 35, 56 and 89 are allowable over the cited reference.

Claims 2-15, 20-24, 28, 29, 32-34, 36-42, 46-49, 53-55, 57-70, 75-78, 82, 83, 86-88, 90-103, 108-112, 116, 117, 120-122,

124-128, and 130, 131 and 133-136 depend from one of independent claims 1, 35, 56, 89, 123, or 132, which are allowable over the cited reference. Therefore, the listed dependent claims are allowable over the cited reference. Reconsideration and notice to that effect is respectfully requested.

Rejections under 35 U.S.C. §103(a)

Claims 16-19, 25-27, 30, 31, 43-45, 50-52, 71-74, 79-81, 84, 85, 104-107, 113-115, 118, 119, and 129 were rejected under 35 U.S.C. §103(a) as being unpatentable over the Diamant patent in view of the Aucsmith patent. The Office Action states that

> "it would have been obvious to a person of ordinary skill in the art to implement the claimed invention by including a method for creating and storing a public-private key as taught by Aucsmith for authenticating data originating from said security partition as taught by Diamant. Such modifications would have been obvious because by combining the teachings of Aucsmith with Diamant, the secure storage device provides access to and from the computer to selected storage areas and communication networks while providing authentication of data by creating and storing public-private key."

(Office Action, p. 45). First, as previously discussed, the Diamant patent does not teach, suggest or disclose "authority records" or "limiting access" "by the operating system" as recited in the independent claims. Specifically, the Diamant patent does not teach, suggest or disclose limiting access to the secured partition by the operating system as recited in the claims, and does not teach, suggest or disclose a security partition containing at least one authority record as recited in the claims. Instead, the Diamant patent utilizes a controller within the operating system environment and outside of the storage device to control access to the secured storage area 18 such that only "access requests which are provided via the secured network 8" are provided access to the secured storage area 18. Though the Diamant patent mentions the use of a key to

encrypt data, the Diamant patent does not mention public-private key pairs.

For the sake of argument, assuming Aucsmith teaches key pairs, the combination of the Diamant patent with the Aucsmith patent still does not teach, suggest, or disclose the claimed invention. The combination would result in a device external to the storage device for controlling access to the secured data area, since both Aucsmith and Diamant disclose devices external to the storage device for controlling access. In both instances, the external device operates within an operating system environment that is within an operating system of, for example, a server 4 (in Diamant). The asserted combination actually teaches away from the claimed invention, because access decisions are rendered by the external device from within the operating system environment. Thus, access to the secured area or security partition by the operating system is not limited. Consequently, the combination of the Aucsmith key pairs with the unrelated security system of the Diamant patent does not teach the claimed invention.

Additionally, it is important to note that in the Diamant patent the controller device (28, 38, 48, 300, or 400 "generates a security key" and provides it to the CPU along with analysis software from the secured area. The Diamant patent reads as follows:

> "The security key is preferably generated according to a momentary data situation in the secured area 32. The security key can also be generated as a one time key which is independent of the secured area 320, such as according to an internal random generator and the like. The main reason for this is to minimize and preferably eliminate all possible access to this security key from elements which are not authorized and which may attempt to try to provide this key to the processor 302."

See Col. 12, line 33 through Col. 13, line 22 (emphasis added). While it is unclear what is meant by momentary data situation, it is clear that the key is intended for temporary storage or

expiration only. By contrast, the Aucsmith patent discloses "a set of keys that are associated with access rights within the computer system" which are stored in access controller unit 106 (*See* Col. 4, lines 37-40). The Aucsmith patent teaches permanent storage of the set of keys in the access controller unit 106. The permanent key storage of the Aucsmith patent cannot be combined with the "momentary data situation" of the Diamant patent without resolving this "permanent versus temporary storage" contradiction. The Diamant patent avoids storing the keys so as to minimize or eliminate unauthorized access to the keys. Consequently, the Diamant patent teaches away from the permanent key storage of the Aucsmith patent. It is not obvious to make the suggested combination, since the Aucsmith patent teaches away from the momentary data situation of the Diamant patent.

Moreover, the Aucsmith patent does not teach public-private key pairs as suggested in the Office Action. The Aucsmith patent reads as follows:

> The keys can either be private symmetric-keys or public asymmetric-keys. The difference is the extent of protection required by the operating system's copy of the key.

See Col. 5, lines 14-16. Thus, it is not clear that the Aucsmith patent even contemplates a public-private key pair, since the keys are either private and symmetric or public and asymmetric.

Additionally, there is no suggestion or teaching in either reference to make the suggested combination. The alleged "obviousness" of the combination of the key pairs of the Aucsmith patent with controller of the Diamant patent constitutes nothing more than a hindsight reconstruction based on the disclosure of the present invention, which discloses key pairs and encryption in combination with security partitions on a storage device, to which access by the operating system is limited. There is no suggestion in either reference to make the asserted combination or to restrict access to a security partition by the operating

system as recited by the claimed invention. None of the cited references alone, or in combination, teach, suggest, or disclose "at least one authority record and at least one data set associated with said authority record" and "limiting access to the security partition of said storage device by said operating system of said computer system" of the claimed invention".

Since the keys in the two references teach away from one another (permanent storage versus "momentary data situation"), since the Aucsmith reference does not teach, suggest, or disclose public-private key pairs, since the asserted combination teaches away from the claimed invention, and since there is no teaching in either reference to make the suggested combination, the combination of the Diamant patent and the Aucsmith patent is inappropriate. The cited combination does not teach, suggest or disclose the claimed invention as recited in claims 16, 17, 25, 43, 44, 71, 72, 79, 104, 105, 113, and 129. The rejection of claims 16, 17, 25, 43, 44, 71, 72, 79, 104, 105, 113, and 129 over a combination of the Diamant patent with the Aucsmith patent under 35 U.S.C. §103(a) is overcome and should be withdrawn

The rejections of claims 16-19, 25-27, 30, 31, 43-45, 50-52, 71-74, 79-81, 84, 85, 104-107, 113-115, 118, 119, and 129 under §103(a), as recited in the Office Action, are all based on the Diamant patent. As previously discussed, the Diamant patent does not teach, suggest or disclose "authority records" or "limiting access" "by the operating system" as recited in the independent claims. The Aucsmith patent, which is combined with the Diamant patent, teaches an access controller unit 106 within the computer 100. As with the Diamant patent, the Aucsmith patent makes no reference to restricting or limiting access to a security partition on the storage device by an operating system. In fact, the access controller unit 106 appears to operate within the operating system environment. Consequently, the cited
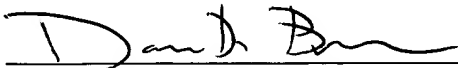
references, alone or in combination, do not teach suggest or disclose "authority records" or "limiting access" "by the operating system" as recited in the claimed invention. Each of claims 16-19, 25-27, 30, 31, 43-45, 50-52, 71-74, 79-81, 84, 85, 104-107, 113-115, 118, 119, and 129 depend from an allowable independent claim. Therefore, all of claims 16-19, 25-27, 30, 31, 43-45, 50-52, 71-74, 79-81, 84, 85, 104-107, 113-115, 118, 119, and 129 are allowable over the cited combination.

CONCLUSION

With this amendment, claim 128 is renumbered as claim 137 and claim 131 is amended to correct a typographical error. New claims 138-145 are added to fully capture the scope of the claimed invention. All of pending claims 1-145 are allowable over the cited art, and reconsideration and notice to that effect is respectfully requested. The Examiner is invited to contact Judson Champlin at the telephone number listed below if such a call would in any way facilitate allowance of this application. The Director is authorized to charge any fee deficiency required by this paper or credit any overpayment to Deposit Account No. 23-1123.

Respectfully submitted,

WESTMAN, CHAMPLIN & KELLY, P.A.

By: _____
David D. Brush, Reg. No. 34,557
Suite 1600 - International Centre
900 Second Avenue South
Minneapolis, Minnesota 55402-3319
Phone: (612) 334-3222 Fax: (612) 334-3312

JKC/RMR:rkp